CLAIMS

What is claimed is:

1. A network system that resists denial of service attacks on an access link to a destination host belonging to a virtual private network (VPN), said network system comprising:

one or more egress boundary routers having connections to an access network including the access link, wherein said one or more egress boundary routers transmit intra-VPN traffic from sources within the VPN and extra-VPN traffic from sources outside the VPN within separate access network logical connections for intra-VPN and extra-VPN traffic; and

a plurality of ingress boundary routers coupled to the one or more egress boundary routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, such that denial of service attacks on said access link originating from sources outside the VPN can be prevented.

2. The network system of Claim 1, and further comprising a Differentiated Services network coupling at least one of the plurality of ingress boundary routers and at least one of the one or more egress boundary routers.

3. The network system of Claim 1, and further comprising a plurality of customer premises equipment (CPE) edge routers each coupled to a respective one of said plurality of ingress boundary routers.

4. The network system of Claim 1, and further comprising the access network.

5. The network system of Claim 4, and further comprising a customer premises equipment (CPE) edge router to the access link.

6. The network system of Claim 5, said CPE edge router having a physical port coupled to said access link, said physical port implementing a first logical port for intra-VPN traffic and a second logical port for extra-VPN traffic.

7. The network system of Claim 1, wherein at least one of said plurality of ingress boundary routers implements a plurality of tunnels that logically partition intra-VPN and extra-VPN traffic.

8. The network system of Claim 1, wherein said one or more egress boundary routers provide a plurality of different qualities of services to said intra-VPN traffic.

9. A network system, comprising:

an access network having an access link to a destination host belonging to a virtual private network (VPN), wherein said access network supports a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN;

one or more egress boundary routers having connections to the access network, wherein said one or more egress boundary routers transmit intra-VPN traffic toward the destination host via the first logical connection and transmit extra-VPN traffic toward the destination host via the second logical connection; and

a plurality of ingress boundary routers coupled to the one or more egress boundary routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, such that denial of service attacks on said access link originating from sources outside the VPN can be prevented.

10. The network system of Claim 9, and further comprising a Differentiated Services network coupling at least one of the plurality of ingress boundary routers and at least one of the one or more egress boundary routers.

11. The network system of Claim 9, and further comprising a plurality of customer premises equipment (CPE) edge routers each coupled to a respective one of said plurality of ingress boundary routers.

12. The network system of Claim 9, and further comprising a customer premises equipment (CPE) edge router to the access link.

13. The network system of Claim 12, said CPE edge router having a physical port coupled to said access link, said physical port implementing a first logical port for intra-VPN traffic and a second logical port for extra-VPN traffic.

14. The network system of Claim 9, wherein at least one of said plurality of ingress boundary routers implements a plurality of tunnels that logically partition intra-VPN and extra-VPN traffic.

15. The network system of Claim 9, wherein said one or more egress boundary routers provide a plurality of different qualities of services to said intra-VPN traffic.

16. A method of protecting an access link to a destination host belonging to a virtual private network (VPN) against denial of service attacks, said method comprising:

in an access network including the access link, providing a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN;

communicating, from a plurality of ingress boundary routers to one or more egress boundary routers, intra-VPN and extra-VPN traffic destined for said destination host, wherein said intra-VPN traffic and said extra-VPN traffic are transmitted utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic;

transmitting intra-VPN traffic from said one or more egress boundary routers toward the destination host via the first logical connection, and transmitting extra-VPN traffic from said one or more egress boundary routers toward the destination host via the second logical connection, such that denial of service attacks on said access link originating from sources outside the VPN can be prevented.

17. The method of Claim 16, wherein said communicating comprises communicating utilizing a Differentiated Services protocol.

18. The method of Claim 16, wherein a customer premises equipment (CPE) edge router is coupled between said access network and said destination host, said method further comprising:

at a physical port of the CPE edge router coupled to the access link, providing first and second logical ports; and

receiving intra-VPN traffic at the first logical port, and receiving extra-VPN traffic at the second logical port.

19. The method of Claim 16, and further comprising logically partitioning intra-VPN and extra-VPN traffic by at least one of said plurality of ingress boundary routers utilizing a plurality of tunnels.

20. The method of Claim 16, and further comprising said one or more egress boundary routers providing a plurality of different qualities of services to said intra-VPN traffic.